AMENDMENTS TO THE CLAIMS

Cancel Claims 1-10 without prejudice. Please accept amended Claims 11 and 22 as follows:

1-10 (Cancelled).

11. (Currently Amended) A method for ensuring that a processor will execute only authorized code, said method comprising:

applying an original digital signature to all authorized code;

storing said signed authorized code in a protected memory, wherein said protected memory is cryptographically protected;

preparing to execute code from the protected memory by verifying a digital signature used to sign said code in accordance with a public key, which corresponds to said original digital signature; and

if said original digital signature is verified, then branching to a copy of said authorized code in said protected memory to begin execution and performing inline decryption of the copy of said authorized code ~~is~~ in said protected memory.

12. (Cancelled)

13. (Original) A method as recited in claim 11 wherein the integrity of the contents of said protected memory is protected by encryption.

14. (Original) A method as recited in claim 11 wherein said protected memory is physically protected.

15. (Original) A method as recited in claim 11 wherein said public key is stored in said protected memory.

16. (Original) A method as recited in claim 11 wherein the integrity of said authorized code is protected at run time.

17. (Original) A method as recited in claim 16 wherein the integrity of said authorized code is protected with symmetric key encryption.

18. (Original) A method as recited in claim 11 wherein the privacy of said authorized code is protected at run time.

19. (Original) A method as recited in claim 18 wherein the privacy of said authorized code is protected at run time with symmetric key encryption.

20. (Original) A method as defined in claim 11, further comprising:

storing code in the protected memory with an original digital signature corresponding to an Owner Public Key; and

verifying the Owner Public Key in accordance with a Manufacturer Public Key, which is resident on the processor, and then verifying the original digital signature in accordance with the Owner Public Key.

21. (Original) A method as defined in claim 20, further comprising:

reading a Certificate containing an Owner Public Key;

validating the Certificate with the Manufacturer Public Key;

finding the Owner Public Key in the Certificate that matches the Owner Number in the processor; and

using the matched Owner Public Key to verify the authorized code.

22. (Currently Amended) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform program steps for ensuring that a processor will execute only authorized code, the program steps comprising:

applying an original digital signature to all authorized code;

storing said signed authorized code in a protected memory, wherein said protected memory is cryptographically protected;

preparing to execute code from the protected memory by verifying a digital signature used to sign said code in accordance with a public key, which corresponds to said original digital signature; and

if said original digital signature is verified, then branching to a copy of said authorized code in said protected memory to begin execution and performing inline decryption of the copy of said authorized code ~~is~~ in said protected memory.